

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
1. September 2005 (01.09.2005)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2005/081089 A1

(51) Internationale Patentklassifikation⁷: **G06F 1/00**

(21) Internationales Aktenzeichen: PCT/EP2005/001817

(22) Internationales Anmeldedatum:
22. Februar 2005 (22.02.2005)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2004 009 065.3
23. Februar 2004 (23.02.2004) DE

(71) Anmelder und

(72) Erfinder: KISTNER, Stefan [DE/DE]; Kölner Strasse 132, 53840 Troisdorf (DE).

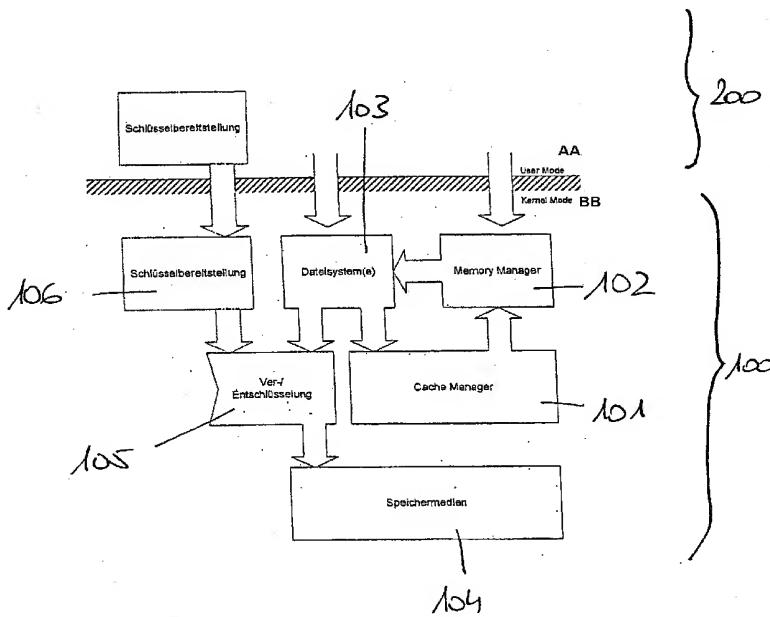
(74) Anwalt: COHAUSZ DAWIDOWICZ HANNIG & PARTNER; Schumannstrasse. 97-99, 40237 Düsseldorf (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR PROTECTING CONFIDENTIAL DATA

(54) Bezeichnung: VERFAHREN ZUM SCHÜTZEN VON VERTRAULICHEN DATEN



- 106 ... KEY PREPARATION
- 103 ... FILE SYSTEM(S)
- 102 ... MEMORY MANAGER
- 105 ... EN-/DECRIPTION
- 101 ... CACHE MANAGER
- 104 ... STORAGE MEDIA
- AA ... USER MODE
- BB ... KERNEL MODE

(57) Abstract: The invention concerns a method for preventing the loss of confidentiality of data electronically stored in a computer system, comprising the following steps: analyzing the protocol and the data flow from and to data carriers and/or peripheral devices; forming a classification, particularly for differentiating between non-exchangeable and exchangeable data carriers; determining, according to the encountered classification, whether an encryption of the electronically stored data is required for preventing the loss of confidentiality of the data and, according to this determination; optionally supplementing the file system on an exchangeable data carrier with a cryptographic encryption and/or carrying out a cryptographic encryption of all or several of the blocks of the exchangeable data carrier.

(57) Zusammenfassung: Verfahren zur Verhinderung des Verlustes der Vertraulichkeit der in einem Computersystem elektronisch gespeicherten Daten mit den Schritten: - Analyse des Protokolls und des Datenstromes von und zu Datenträgern und/oder Peripheriegeräten; - Bildung einer Klassifikation, insbesondere zur Unterscheidung zwischen nicht wechselbaren sowie wechselbaren Datenträgern - Festlegung in Abhängigkeit

der getroffenen Klassifikation, ob eine Verschlüsselung der elektronisch gespeicherten

[Fortsetzung auf der nächsten Seite]

WO 2005/081089 A1



MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten** (*soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL,

PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

VERFAHREN ZUM SCHUTZEN VON VERTRAULICHEN DATEN

Die Erfindung betrifft ein Verfahren zur Verhinderung des Verlustes der Vertraulichkeit der in einem Computersystem elektronisch gespeicherten Daten, wobei die Daten insbesondere mittels eines Dateisystems verwaltet werden und/oder eine Einteilung in Blöcke erfolgt, insbesondere bei Verwendung wechselbarer und/oder austauschbarer Datenträger und/oder Speichermedien, wobei an das Computersystem insbesondere Peripheriegeräte anschließbar sind.

Arbeitsplatzcomputer verfügen zunehmend über Schnittstellen, über die ein unkontrollierter und in der Regel unerwünschter Datenaustausch mittels wechselbarer und/oder austauschbarer Datenträger und/oder Speichermedien stattfinden kann. Die Abschaltung dieser Schnittstellen ist nicht praktikabel, da sie wie zum Beispiel die USB-Schnittstelle zum Anschluss von Peripheriegeräten erwünscht sind.

Der Transport und die Aufbewahrung wechselbarer Datenträger und Speichermedien erfordern besondere Sicherheitsmaßnahmen, um ein unbefugtes Lesen und damit den Verlust der Vertraulichkeit zu verhindern. Bekannt ist die Anwendung kryptografischer Verschlüsselungsverfahren zur Verschlüsselung der Daten, um ein unbefugtes Lesen der Daten zu verhindern.

Problematisch ist dabei, dass es bei den bekannten Arbeitsplatzcomputern möglich ist, ohne spezifische technische Kenntnisse Speichermedien an Computern anzuschließen. Mit der quasi ubiquitären Verfügbarkeit nimmt die Gefahr des missbräuchlichen Einsatzes stetig zu. Dieser Gefahr stehen keine administrativen Kontrollmechanismen gegenüber.

Insbesondere die an modernen Computersystemen vorhandene USB-Schnittstelle stellt eine Gefahr dar, da an USB-Schnittstellen anschließbare, sogenannte Memory Sticks sehr klein und unauffällig und einfach zu handhaben sind und bei modernen Betriebssystemen auch bei bereits eingeschaltetem Computer unmittelbar erkannt werden. Derartige Speichermedien gestatten somit auf sehr einfache Weise einen Missbrauch, das heißt insbesondere des Diebstahls von elektronisch gespeicherten Daten.

Aus WO 02/19592 A2 ist ein Verfahren bekannt, bei dem auf einem UNIX basierten System jede Datei, die auf einem Speichermedium wie Diskette oder CD-ROM gespeichert werden soll, blockweise verschlüsselt wird, und wobei eine zu lesende verschlüsselte Datei automatisch blockweise entschlüsselt wird.

Nachteilig dabei ist, dass bei einer generellen Verschlüsselung bei jedem Speichervorgang ein erwünschter Datentransfer, beispielsweise für Veröffentlichungen, unterbunden wird. Weiterhin nachteilig ist bei diesem Verfahren, dass eine Unterscheidung zwischen verschiedenen Datenträgern hinsichtlich der potentiellen Gefahr eines Datenverlustes nicht getroffen werden kann.

Aufgabe der Erfindung ist es, diese Nachteile zu überwinden und ein Verfahren zu schaffen, welches unter Beibehaltung der Schnittstellenfunktionalität den unerwünschten Datentransfer mittels wechselbarer Speichermedien verhindert, ohne den erwünschten Datentransfer mittels wechselbarer Speichermedien einzuschränken.

Diese Aufgabe wird erfindungsgemäß dadurch gelöst, dass bei einem Verfahren zur Verhinderung des Verlustes der Vertraulichkeit der in einem Computersystem

elektronisch gespeicherten Daten, wobei die Daten insbesondere mittels eines Dateisystems verwaltet werden und/oder eine Einteilung in Blöcke erfolgt, insbesondere bei Verwendung wechselbarer und/oder austauschbarer Datenträger und/oder Speichermedien, wobei an das Computersystem insbesondere Peripheriegeräte anschließbar sind, die folgenden Schritte durchgeführt werden:

- Analyse des Protokolls und des Datenstromes von und zu Datenträgern und/oder Speichermedien und/oder Peripheriegeräten;
- Bildung einer Klassifikation, insbesondere zur Unterscheidung zwischen nicht wechselbaren sowie wechselbaren Datenträgern und/oder Speichermedien;
- Festlegung in Abhängigkeit der getroffenen Klassifikation, ob eine Verschlüsselung der elektronisch gespeicherten Daten zur Verhinderung des Verlustes der Vertraulichkeit der Daten erforderlich ist und in Abhängigkeit dieser Festlegung gegebenenfalls
- Ergänzen des Dateisystems auf einem wechselbaren Datenträger und/oder einem wechselbaren Speichermedium um eine kryptografische Verschlüsselung und/oder Durchführung einer kryptografischen Verschlüsselung aller oder einiger Blöcke des wechselbaren Datenträgers und/oder des wechselbaren Speichermediums.

Durch das erfindungsgemäße Verfahren ist somit in besonders vorteilhafter Weise möglich, den Verlust der Vertraulichkeit der in einem Computersystem elektronisch gespeicherten Daten zuverlässig zu verhindern und dabei eine größtmögliche Flexibilität der Gestalt zu ermöglichen, da unter Beibehaltung der Schnittstellenfunktionalität der unerwünschte Datentransfer mittels wechselbarer Datenträger und/oder Speichermedien verhindert wird, wobei der erwünschte Datentransfer nicht eingeschränkt wird. Besonders vorteilhaft ist dabei, dass verfahrensgemäß eine Klassifikation der Datenträger bzw. Speichermedien durchgeführt wird und insbesondere zwischen Typen von Datenträgern und/oder Speichermedien unterschieden werden kann.

Weitere vorteilhafte Ausgestaltungen des erfindungsgemäßen Verfahrens sind in den Unteransprüchen angegeben.

Ein in das Betriebssystem eingebundenes Programm, in der Regel bestehend aus mehreren Treibern, Filtern, Diensten etc., analysiert Protokoll und Datenstrom von und zu Datenträgern, Speichermedien und Peripheriegeräten. Unter Einbeziehung der a priori bekannten ausgewiesenen oder administrativ deklarierten Eigenschaften und Präferenzen erfolgt eine selbstständige Klassifikation hinsichtlich der Möglichkeit, als wechselbares Speichermedium bzw. als wechselbarer Datenträger zu dienen, um somit eine Festlegung zu treffen, ob die Gefahr des Verlustes der Vertraulichkeit der Daten besteht und somit gegebenenfalls eine Verschlüsselung der Daten durchzuführen.

Insbesondere können alle als wechselbare Speichermedium tauglichen Datenträger oder Geräte mit einer Verschlüsselung belegt werden. Es kann entweder der Datenträger als ganzes oder alternativ lediglich Dateiinhalte oder Teile der Dateien oder ausgewählte Dateien verschlüsselt werden.

Datenträger oder Speichermedium im Sinne dieses Verfahrens ist insbesondere jeder nicht flüchtige Speicher, der von Computersystemen lesbar oder lesbar und beschreibbar ist. Er kann fest oder wechselbar mit dem Computer verbunden sein und/oder über wechselbare Medien verfügen, wie beispielsweise Disketten, ZIP-Laufwerke, Jaz, Bänder, CD, MO, WORM etc.

Die Organisation nicht flüchtiger Datenträger erfolgt typischerweise in Blöcken bzw. Sektoren. Die Blöcke sind bei den meisten Datenträgern von konstanter Größe, insbesondere der Größe 2^n mit n größer als 8. Sie können aber auch von variabler Größe sein, zum Beispiel bei Streamern. Die physikalische Realisation, das heißt elektrisch, magnetisch, optisch etc., und die Verteilung der Blöcke auf dem Datenträger ist für die Anwendung des erfindungsgemäßen Verfahrens unerheblich. Blöcke bilden dabei die kleinste lesbare oder schreibbare Einheit.

Die Abstraktion einer Partition oder eines nicht zu partitionierenden Datenträgers ist ein Volume. Dabei handelt es sich um die Entität der mit Hilfe eines Dateisystems verwalteten Blöcke. Es kann einen oder mehrere Datenträger oder Partitionen umfassen. Jedes Volume verfügt über eine integrale Anzahl von

Blöcken. Ein Volume wird durch einen Mount-Vorgang zugänglich gemacht und steht bis zum Unmount zur Verfügung innerhalb des Computersystems. Bei Verwendung beispielsweise von Memory Sticks, die an USB-Anschlüsse angeschlossen werden können, erfolgt der Mount-Vorgang automatisch, da moderne Betriebssysteme von Computersystemen derartige Peripheriegeräte unmittelbar erkennen.

Auf Volumes, das heißt insbesondere auf Partitionen oder einem gesamten Datenträger abgelegte Daten werden mit einem Dateisystem organisiert. Dieses Dateisystem verwaltet die Dateien sowie Metainformationen über die Dateien, die erforderlich sind, um die Daten auf dem Datenträger zu lokalisieren. Die Daten selbst sind in Dateien organisiert. Die Metainformationen sind in Verzeichnissen und gegebenenfalls weiteren Dateien, die im allgemeinen nicht zugänglich sind, abgelegt. Es ist eine Vielzahl von Dateisystemen mit zum Teil weiteren spezifischen Eigenschaften bekannt. Jedes Dateisystem bildet die logische Organisation eines Datenträgers in spezifischer Art und Weise auf die zu Grunde liegende Blockstruktur des Datenträgers ab.

Betriebssysteme unterscheiden zwischen mindestens zwei Hierarchieebenen, in denen Software ausgeführt wird. Im (privilegierten) Kernel Mode sind alle Maschinenbefehle ausführbar, d.h. der Zugriff auf Systemdaten und Hardware ist nahezu uneingeschränkt möglich. Der in diesem Modus betriebene Betriebssystemkern abstrahiert und virtualisiert die Hardware und stellt Dienste für den im User Mode laufenden Teil des Betriebssystems bereit. Dieser arbeitet in einem nicht (oder weniger) privilegierten Prozessormodus, d.h. es steht nur ein eingeschränkter Satz von Maschinenbefehlen zur Verfügung. Der Zugriff auf Systemdaten und Hardware ist in der Regel nicht möglich. Anwendungen und geschützte Subsysteme laufen im User Mode.

Das vorgestellte Verfahren kann die modulare Struktur heutiger Betriebssysteme ergänzen. Es kooperiert mit dem Betriebssystem und erweitert es. Dabei ist es nicht erforderlich, Teile des Betriebssystems zu ersetzen oder zu modifizieren. Es wird lediglich die Arbeitsweise von Dateisystemtreibern modifiziert, indem die binäre Repräsentation der Daten auf dem Datenträger verändert wird.

Das Verfahren ist insbesondere für alle Betriebssysteme die mit Datenträgern mit Blockstruktur arbeiten anwendbar.

Alle als wechselbares Speichermedium tauglichen Datenträger oder Geräte können somit in Abhängigkeit der vorgenommenen Klassifikation mit einer Verschlüsselung belegt werden. Dabei kann entweder der Datenträger als ganzes oder lediglich Dateiinhalte verschlüsselt werden.

Das erfindungsgemäße Verfahren ermöglicht die Benutzung wechselbarer Speichermedien, ohne dass befürchtet werden muss, dass diese von Unbefugten kompromittiert werden können. Dies gilt nicht nur für Halbleiterspeicher wie wechselbare Festplatten, Memory Sticks etc., sondern auch für alle magnetischen, magnetooptischen oder optischen Datenträger wie beispielsweise Diskette, ZIP-Laufwerk, Jaz, Bänder, CD, MO, WORM etc. Es ist nicht erforderlich, Schnittstellen oder Laufwerke abzuschalten oder gar auszubauen. Damit kann die volle Funktionalität der Computerhardware genutzt werden.

Das erfindungsgemäße Verfahren wird auf einer sehr niedrigen Ebene quasi unmittelbar vor dem Datenträger angewandt, so dass das erfindungsgemäße Verfahren weder für Anwendungsprogramme noch für das Betriebssystem in Erscheinung tritt. Insbesondere erfolgt nicht zwangsläufig eine Kopplung von Benutzerauthentifizierung und Schlüsselmanagement. Dies macht die Sicherheit der Speichermedien unabhängig von der Sicherheit des Betriebssystems, das heißt unsichere, ausgespähte oder notierte Passworte vermindern die Sicherheit nicht.

Es ist keine Aktion seitens der Benutzer erforderlich, welche durch Fahrlässigkeit oder böse Absicht unterbleiben könnte.

Es ist keine Änderung in der Logik des Betriebssystems oder ein spezielles Dateisystem wie beispielsweise EFS Encrypting File System erforderlich. Die spezifischen Vorteile des jeweiligen Dateisystems bleiben im vollen Umfang erhalten, da auf das Dateisystem an sich kein Einfluss genommen wird. Der

Schutz ist nicht an ein bestimmtes Dateisystem gebunden, sondern ergänzt jedes Dateisystem.

Bei Verlust oder Entwendung von Datenträgern bedeutet dies nicht zugleich den Verlust der Vertraulichkeit der darauf enthaltenen Daten, da diese auf dem Datenträger gespeicherten Daten vollständig oder zumindest teilweise verschlüsselt sind. Das zur Anwendung kommende kryptografische Verfahren bleibt einem potentiellen Angreifer unbekannt, womit ein Angriff erschwert wird.

Somit wird unter Anwendung eines erfindungsgemäßen Verfahrens aus einem potentiell unsicheren Speichermedium ein Speichermedium für besondere Sicherheitsanforderungen, denn besonders sensible Daten können ausschließlich auf wechselbaren Speichermedien gehalten werden, um durch physischen Verschluss vor unbefugtem Zugriff geschützt zu werden.

Durch Anwendung des erfindungsgemäßen Verfahrens auf mehreren Computern unter Verwendung eines gemeinsamen Schlüssels entsteht eine Sicherheitsdomäne. Dabei ist es nicht erforderlich, dass die Computer einer Sicherheitsdomäne miteinander verbunden sind, wie beispielsweise in einem Netzwerk (LAN, WAN). Innerhalb einer Sicherheitsdomäne wird die Verschlüsselung wechselseitig aufgehoben, so dass wechselbare Speichermedien, beispielsweise zur Datensicherung, uneingeschränkt verwendet werden können. Die vom Betriebssystem zur Verfügung gestellten Mittel der Zugriffskontrolle bleiben dabei erhalten.

Vorzugsweise ist festlegbar, dass eine Verschlüsselung aller Blöcke des Datenträgers/Speichermediums oder dass eine Verschlüsselung aller Dateien von der Speicherung auf dem Datenträger/Speichermedium oder dass eine Verschlüsselung einiger Dateien vor der Speicherung auf dem Datenträger/Speichermedium erfolgt.

Hierdurch ist es in vorteilhafter Weise möglich, eine gestufte Sicherheits- und Kompatibilitätshierarchie zu schaffen, in der hinsichtlich der zu speichernden Daten eine Klassifikation erfolgen kann.

Bei einer Verschlüsselung aller Blöcke des Datenträgers, das heißt bei einer Verschlüsselung des gesamten Volumes, werden alle Sektoren verschlüsselt. Der Datenträger erscheint auf Computersystemen ohne das erfindungsgemäße Verfahren randomisiert, das heißt unformatiert und somit nicht lesbar. Diese Strategie bietet maximale Sicherheit bei minimaler Kompatibilität.

Alternativ kann eine Verschlüsselung aller Dateien des Volumes, das heißt aller Dateien einer Partition oder eines Datenträgers, erfolgen. Der Datenträger bzw. das Volume erscheint somit auf Computersystemen, ohne das erfindungsgemäße Verfahren intakt, wobei die Dateien selbst randomisiert erscheinen, das heißt nicht lesbar sind. Der Versuch eines Zugriffs führt zu Fehlermeldungen und ist erfolglos. Lediglich die Dateinamen können Hinweise auf den Inhalt bieten, der jedoch verborgen bleibt.

Alternativ kann eine Verschlüsselung einiger ausgewählter Dateien eines Volumes erfolgen. Neu angelegte oder überschriebene oder festlegbaren Kriterien folgende Dateien werden verschlüsselt. Als solche Kriterien können insbesondere Dateityp und Speicherort dienen. Bereits bestehende Dateien bleiben unverändert. Insbesondere können bestehende Dateien mit einem nicht aufzuhebenden Schreibschutz versehen werden, so dass Änderungen an ihnen ausgeschlossen sind. Vorteilhaft bei dieser Strategie ist insbesondere eine hohe Sicherheit bei maximaler Kompatibilität zu Rechnern oder Geräten ohne das erfindungsgemäße Verfahren. Beispielsweise erzeugen Digitalkameras unverschlüsselte Dateien auf einem Volume, in diesem Fall dem Kameraspicher, die gelesen werden können. Alle schreibenden Dateizugriffe erfolgen jedoch verschlüsselt.

Insbesondere ist es bei der Verschlüsselung einiger ausgewählter Dateien vor der Speicherung auf dem Datenträger/Speichermedium möglich, die Metadaten bzw. die Kommunikation als Gesamtheit zu erhalten, die Daten an sich jedoch vor einem Zugriff zu schützen.

Alternativ oder kumulativ ist es auch möglich, dass jedes Dateisystem auf nicht wechselbaren und/oder nicht austauschbaren Datenträgern und/oder Speichermedien um eine kryptografische Verschlüsselung ergänzt wird. Hierdurch kann eine maximale Sicherheit erreicht werden.

In einer bevorzugten Ausführungsform wird die kryptografische Verschlüsselung bei Vorliegen besonderer Merkmale temporär außer Kraft gesetzt. Dieses kann insbesondere dadurch realisiert werden, dass eine Hardware mit einem eingebundenen Schlüssel wie beispielsweise ein Dongle und/oder unter Verwendung eines Kennwortes und/oder durch Erkennung und Überprüfung biometrischer Daten eines Benutzers einer Verschlüsselung von Daten unterbindbar ist, um beispielsweise eine gewünschte Veröffentlichung von Daten zu ermöglichen.

Bei Verwendung eines Datenträgers und/oder eines Speichermediums ohne Dateisystem kann eine Verschlüsselung aller Blöcke erfolgen.

Bei Anschluss eines Datenträgers und/oder Speichermediums an eine multifunktionale Schnittstelle und/oder einen multifunktionalen Bus, insbesondere Steckplatz, USB-Schnittstelle und dergleichen, bleibt die Schnittstellen- und/oder Bus-Funktionalität voll erhalten und es werden nur derartige Datenströme zumindest teilweise einer Verschlüsselung unterworfen, die zur Abspeicherung der Daten an die Schnittstelle und/oder den Bus weitergeleitet werden. Ein Erkennen dieser Datenströme ist durch das erfindungsgemäße Verfahren gewährleistet, da eine Analyse des Datenstroms von und zu Datenträgern und/oder Speichermedien und/oder Peripheriegeräten erfolgt. Hierdurch kann es gewährleistet werden, dass einerseits die volle Schnittstellen- oder Bus-Funktionalität erhalten bleibt, wie dies beispielsweise bei Anschluss eines Druckers an eine USB-Schnittstelle erforderlich ist, und andererseits bei zu speichernden Daten, wie dies bei Anschluss eines Memory-Sticks an eine USB-Schnittstelle der Fall ist, eine zumindest teilweise automatische Verschlüsselung zur Verhinderung des Verlustes der Vertraulichkeit der Daten durchgeführt wird.

Vorzugsweise erfolgt eine Analyse der Schnittstelle und/oder des Busses, an die der Datenstrom erfolgen soll, wobei diese Analyse bei der Bildung der Klassifikation insbesondere anhand festlegbarer Kriterien berücksichtigt wird, insbesondere hinsichtlich der physikalischen Verbindung und/oder weiterer Eigenschaften, wie beispielsweise mit oder ohne Kabel und/oder Geräteeigenschaften und/oder intern bzw. extern und/oder fest bzw. wechselbar, das heißt, dass beispielsweise Drucker und Memory Sticks, die gleichermaßen über eine USB-Schnittstelle mit dem Computersystem verbindbar sind, unterschiedlich klassifizierbar sind hinsichtlich der Gefahr eines Verlustes der Vertraulichkeit der Daten.

Vorzugsweise werden zur Verschlüsselung kryptografische Methoden angewendet, insbesondere der Rijndael-Algorithmus bietet eine hohe Sicherheit gegen eine unbefugte Entschlüsselung.

Bei einem Lesevorgang von einem zumindest teilweise verschlüsselten Datenträger und/oder Speichermedium erfolgt vorzugsweise automatisch eine Entschlüsselung der Daten. Vorteilhaft ist es, wenn bei Zugriff auf einen Datenträger und/oder Speichermedium eine Prüfung erfolgt, ob eine Verschlüsselung aller Blöcke des Datenträgers / Speichermediums oder eine Verschlüsselung aller Dateien auf dem Datenträger / Speichermedium oder eine Verschlüsselung einiger Dateien vorliegt, und dass eine Entschlüsselung der angeforderten Daten erfolgt.

Zur Verschlüsselung bzw. Entschlüsselung können Schlüssel Verwendung finden, die durch Zusammensetzung verschiedener Anteile gebildet sind, wobei insbesondere mehrere Computersysteme zu Gruppen zusammengefasst werden, wobei die Schlüssel einer Gruppe von Computersystemen einen übereinstimmenden Anteil sowie jeweils einen individuellen Anteil aufweisen.

Insbesondere ist eine Schlüsselbildung durch Zusammensetzung verschiedener Anteile variabler oder fester BIT-Länge möglich. Durch ein Schlüsselmanagement in Art einer Schließanlage können Sicherheitsdomänen organisiert werden. Des Weiteren ist die Bildung von Schlüsselmengen als

Unterschlüssel einer Sicherheitsdomäne möglich, wobei Schnittmengen gebildet werden können, derart, dass ein Austausch von Daten, das heißt die Entschlüsselung verschlüsselter Daten innerhalb einer Gruppe, freigegeben oder unterbunden oder teilweise unterbunden werden kann.

Der Schlüssel kann einerseits innerhalb des erfindungsgemäßen Verfahrens implementiert, das heißt fest kodiert sein. Der Schlüssel kann jedoch auch in einer Datenbank abgelegt sein, oder in einer Hardware eingebunden sein, beispielsweise in einem Dongle oder unter Verwendung eines Algorithmus aus biometrischen Daten eines Benutzers ermittelt werden.

Eine Implementation des erfindungsgemäßen Verfahrens kann dergestalt erfolgen, dass eine Kombination aus geeigneten Filtern und Treibern erstellt wird, die auf sehr niedriger Ebene den Protokoll- und Datenfluss zwischen den Anwendungsprogrammen und höheren Ebenen des Betriebssystems einerseits und den Speichermedien andererseits analysiert und - nach Bedarf - modifiziert.

Die Modifikation besteht in der Anwendung einer kryptografischen Verschlüsselung. Sie kann (je nach installierter Option) entweder das Speichermedium als Ganzes, oder Teile davon (Dateiinhalte) verschlüsseln. Bei der Verschlüsselung von Teilen (Dateiinhalten) können insbesondere auch die Metadaten manipuliert werden. Die Auswahl der zu überwachenden Schnittstellen und Laufwerke kann produktspezifisch festgelegt oder administrabel sein.

Ein weiteres Modul fungiert als Schlüsselverwalter für die kryptografische Komponente. Er kann für einzelne Computer die notwendigen Schlüssel in einer geeigneten Datei oder Datenbank verwalten. Für mehrere Computer mit gemeinsamer Schlüsselverwaltung stellt dieser Dienst die Schlüssel entweder ebenfalls aus lokaler Verwaltung zur Verfügung, oder - bei Verbindung beispielsweise im LAN - in Abstimmung mit einem zentralen Schlüsselverwalter.

Bei Vorliegen besonderer Merkmale kann die Verschlüsselung temporär außer Kraft gesetzt werden. Diese Merkmale können durch eine besondere

Identifikation - beispielsweise eines physischen Schlüssels - vorliegen; sie können aber auch in den Daten begründet sein. So kann ein sog. Dongle, der nur zeitweise ausgegeben wird, die Verschlüsselung aufheben, um die Erstellung von Datenträgern zur Veröffentlichung zu ermöglichen. Ebenso kann die Erkennung bestimmter Dateiformate die Verschlüsselung aufheben, so dass Bilddaten von einer Kamera gelesen werden können.

Ein Ausführungsbeispiel der Erfindung ist in den Figuren dargestellt und wird im Folgenden näher erläutert. Es zeigen:

Figur 1 Schematische Darstellung der Anwendung des Verfahrens bei mehreren Computersystemen bzw. Computern

Figur 2 Durchführung des Lesens und Schreibens von Daten bei Computersystemen nach dem Stand der Technik

Figur 3 Durchführung des Lesens und Schreibens von Daten bei Computersystemen gemäß einer Ausführungsform des erfindungsgemäßen Verfahrens

Figur 4 Schematische Darstellung des Verfahrens nach Figur 3 mit weiteren Komponenten

Figur 5 Darstellung eines Datenträgers bzw. eines Speichermediums real und aus Sicht zugreifender Programme

Figur 6 Ablauf des Öffnens bzw. Erstellens einer Datei

Figur 7 Datenfluss beim Lesen und Schreiben einer Datei mit dem erfindungsgemäßen Verfahren sowie nach dem Stand der Technik

Figur 8 Datenfluss gemäß Figur 7, jedoch unter Umgehung eines Systemcaches

Figur 9 Datenfluss beim Lesen und Schreiben mittels MMF (Memory Mapped Files)

Figur 10 Schematische Darstellung eines Verschlüsselungsvorgangs

Figur 1 zeigt eine schematische Darstellung der Anwendung des Verfahrens bei mehreren Computersystemen bzw. Computern. Durch Zusammenschluss mehrerer Computer 11, 12, 13 mit gemeinsamer Schlüsselverwaltung entsteht eine Sicherheitsdomäne 10. Dabei ist es nicht notwendig, dass alle Computer 11, 12, 13 miteinander vernetzt sind. So können eine oder mehrere Abteilungen eines Betriebes eine Sicherheitsdomäne 10 bilden. Ebenso können dies mehrere Computer eines Benutzers an unterschiedlichen Standorten sein, zwischen denen Daten per Wechseldatenträger übertragen werden.

Wechselbare Speichermedien 22, die innerhalb der Domäne 10 erstellt werden, bzw. einzelne Dateien darauf, die innerhalb der Domäne 10 geschrieben werden, sind mit Computern 31, 32 außerhalb nicht lesbar und umgekehrt. Innerhalb der Domäne 10 können wechselbare Speichermedien 21 freizügig benutzt werden.

Denkbar sind bei der Anwendung des Verfahrens insbesondere folgende Szenarien:

- Bandkassetten oder andere zur Datensicherung eingesetzte Speichermedien können dezentral aufbewahrt werden. Besondere Transportsicherungsmaßnahmen entfallen.
- Besonders sensible Daten können ausschließlich auf Wechselfestplatten gehalten werden. Sie können physisch weggeschlossen werden und sind nur innerhalb der Sicherheitsdomäne lesbar.
- Gesetzliche Auflagen hinsichtlich des Datenschutzes lassen sich leichter einhalten, da alle Speichermedien, die die Sicherheitsdomäne verlassen oder zwischen nachgeordneten Subdomänen ausgetauscht werden vor unbefugtem Lesen geschützt sind.

- Persönliche oder wirtschaftliche Nachteile können aus dem gleichen Grund vermieden werden.
- In einem LAN können lokale Datensicherungen (auf Clientcomputern) durchgeführt werden. Eine missbräuchliche Nutzung ist nicht zu befürchten.
- Die unkontrollierte Ausführung nicht freigegebener Programme kann unterbunden werden, da der Eintrag via Speichermedien nicht möglich ist (sofern nicht beispielsweise CD-ROMs freigegeben sind).

In Figur 2 dargestellt ist schematisch die Durchführung des Lesens und Schreibens von Daten bei Computersystemen nach dem Stand der Technik. Betriebssysteme unterscheiden dabei zwischen mindestens zwei Hierarchieebenen in denen Software ausgeführt wird. Diese Hierarchieebenen sind zum einen der Kernel-Mode 100 sowie der User-Mode 200. Im User-Mode 200 werden insbesondere Anwendungsprogramme bereitgestellt und ausgeführt.

Im Kernel-Mode werden die im Cache 101 elektronisch zwischengespeicherten Daten über einen Memory-Manager 102 mittels des Dateisystems 103 den Speichermedien 104 zugeführt und auf diesen Speichermedien 104 abgespeichert. Die Anforderung zur Durchführung dieses Vorganges erfolgt durch im User-Mode 200 ausgeführte Anwendungsprogramme. Die entsprechenden Anforderungen solcher Anwendungsprogramme können erfolgen durch Zugriffe entsprechend Pfeil 201, durch Zugriff auf den Memory-Manager 102, oder angedeutet durch den Pfeil 202 durch Zugriff auf das Dateisystem 103. Ein Lesevorgang erfolgt durch eine entsprechende Umkehrung, d.h. durch Auslesen von Daten aus dem Speichermedium 104 über das Dateisystem 103 und gegebenenfalls Weiterleitung der Daten an den Cache-Manager 101, bzw. den Memory-Manager 102.

Die auf den Speichermedien 104 abgelegten Daten sind gegen einen unbefugten Zugriff nicht geschützt. Handelt es sich bei den Speichermedien 104 um wechselbare Speichermedien wie beispielsweise Disketten oder CD, so ist ein Verlust der Vertraulichkeit der Daten nicht auszuschließen.

In Figur 3 dargestellt ist die Durchführung des Lesens und Schreibens von Daten bei Computersystemen, gemäß einer Ausführungsform des erfindungsgemäßen Verfahrens.

Auf der hierarchischen Ebene des Kernel-Modes ist der Kommunikationsstrang zwischen Dateisystem 103 und Speichermedium 104 ergänzt durch eine Verschlüsselung 105. Die Ver-, bzw. Entschlüsselung 105 basiert auf einem von einem Modul 106 bereitgestellten Schlüssel. Bei Vorliegen einer entsprechenden Klassifikation des anzusprechenden Speichermediums 104 erfolgt durch das Ver-, bzw. Entschlüsselungsmodul 105 eine Ver- bzw. Entschlüsselung der zu lesenden, bzw. zu schreibenden Daten.

Das Modul zur Schlüsselbereitstellung 106 ist dabei in der Hierarchieebene des Kernel-Modes 100 implementiert. Dem Schlüsselbereitstellungsmodul 106 können jedoch benutzerdefinierte und/oder Hardware basierte Schlüssel zugeführt werden, aus dem User-Mode 200 beispielsweise unter Verwendung eines Dongles oder unter Verwendung zu erfassender biometrischer Daten des Benutzers.

Eine Implementation des erfindungsgemäßen Verfahrens kann durch die Komponenten gemäß Figur 4 realisiert werden, welche die Kommunikation der Module innerhalb des Betriebssystems beobachten und an geeigneter Stelle modifizieren. Sie erfolgt vorzugsweise vollständig im Kernel Mode 100 gemäß Figur 4. So ist einerseits eine vollständige, nahtlose Integration im Betriebssystem möglich und andererseits der Schutz vor Programmen im User Mode 200 zu erreichen.

Das erfindungsgemäße Verfahren wirkt so, dass die Ver- bzw. Entschlüsselung 105 unmittelbar vor dem Schreiben bzw. nach dem Lesen von Blöcken auf bzw. vom Speichermedium 104 stattfindet. Die auf dem Datenträger 104 möglicherweise verschlüsselt vorliegenden Daten liegen im Hauptspeicher immer unverschlüsselt vor. Dadurch ist selbst bei prozessorintensiven Verschlüsselungsalgorithmen die Beeinträchtigung der Systemleistung minimal. Die Ver- und Entschlüsselung kann besonders vorteilhaft in etwa in der Zeit

durchgeführt werden, zu denen das System ohnehin auf die Erfüllung einer Anforderung an einen Datenträger 104 wartet.

Schreibvorgänge erfolgen dergestalt, dass jeder folgende Block in der Zeit verschlüsselt wird, in welcher der vorhergehende auf den Datenträger 104 geschrieben wird. Analog bei Lesevorgängen, hier wird jeder Block in der Zeit entschlüsselt wird, in welcher der nächste gelesen wird. Vorteilhaft ist dabei, dass bei einer Referenzimplementation selbst PC mit 300 MHz CPU außer einer nicht wahrnehmbaren Latenz keine Verlangsamung zeigen. Die Verwendung des Verfahrens zeigt sich lediglich in der auf ca. 60% angestiegenen CPU Auslastung, anstelle des Leerlaufs während der I/O Wartezeiten.

Das erfindungsgemäße Verfahren lässt an dieser Stelle mehrere Strategien für den Umfang der Verschlüsselung zu. Es bestehen die Möglichkeiten der Verschlüsselung des Datenträgers in toto, d.h. jeder Block wird verschlüsselt oder der Verschlüsselung aller Dateien oder der Verschlüsselung einiger Dateien, wie nachfolgend erläutert wird:

1. Verschlüsselung der Volumes in toto.

Alle Sektoren werden verschlüsselt. Der Datenträger 104 erscheint auf Rechnern ohne dieses Verfahren randomisiert; d.h. unformatiert. Fremde Datenträger 104 müssen vor der Verwendung erst neu formatiert oder bei gewünschtem Datenerhalt konvertiert werden. Zur Erhöhung der Sicherheit kann die Generierung der Initialisierungsvektoren 4010, 4020 (Figur 10) durch die bei diesem Verfahren bekannte absolute Blockadresse (des Datenträgers) modifiziert werden. Diese Strategie bietet maximale Sicherheit bei minimaler Kompatibilität.

2. Verschlüsselung aller Dateien der Volumes.

Der Datenträger 104 erscheint auf Rechnern ohne dieses Verfahren intakt; die Dateien selbst erscheinen randomisiert. Der Zugriff führt zu Fehlermeldungen und ist erfolglos. Lediglich die Dateinamen können Hinweise auf den Inhalt bieten. Bei der Einrichtung müssen alle Dateien verschlüsselt werden.

3. Verschlüsselung einiger Dateien eines Volumes.

Neu angelegte oder überschriebene Dateien werden verschlüsselt. Bereits bestehende Dateien bleiben unverändert. Sie werden mit einem nicht aufzuhebenden Schreibschutz versehen, der vergleichbar ist mit Dateien auf CD-ROM, so dass Änderungen an ihnen ausgeschlossen sind.

Diese Strategie bietet die meisten Vorteile. Die Sicherheit ist bei gut gewähltem kryptographischem Algorithmus hinreichend groß bei maximaler Kompatibilität zu Rechnern oder Geräten ohne dieses Verfahren. Beispielsweise erzeugen Digitalkameras unverschlüsselte Dateien auf einem Volume, d.h. dem Kameraspicher, die gelesen werden können. Alle schreibenden Dateizugriffe erfolgen jedoch verschlüsselt.

Im letztgenannten Modus der Verschlüsselung aller Dateien muss für jede Datei ein Kennzeichen hinsichtlich ihrer Verschlüsselung untergebracht werden. Dabei muss dieses Kennzeichen kompatibel mit allen Dateisystemen bleiben. Mit einer willkürlichen Aufteilung des Namensraumes für Dateinamen ermöglicht dieses Verfahren die Kennzeichnung der mit diesem Verfahren behandelten, d.h. verschlüsselten Dateien entsprechend der Zugehörigkeit des Dateinamens zu einem der beiden Namensunterräume zur Unterscheidung „verschlüsselt“ bzw. „unverschlüsselt“.

Diese Kennzeichnung kann wie im nachfolgenden Beispiel angegeben erfolgen:

Aktion	Darstellung des Dateinamens in einer Anwendung	Dateiname auf dem Datenträger
Datei wird erzeugt	xy.doc	
Das Verfahren modifiziert den Dateinamen		xy.doc.\$~#
Auflistung des Inhaltsverzeichnisses zeigt	xy.doc	
Auflistung des Inhaltsverzeichnisses eines Computersystems ohne das Verfahren zeigt		xy.doc.\$~#

Unter Anwendung des erfindungsgemäßen Verfahrens bleibt somit die Modifikation der Dateien auf einem Datenträger für den Benutzer verborgen, da die Darstellung des Datenträgerinhaltes gemäß dem vorstehenden Beispiel dem Benutzer keinen Hinweis auf eine Manipulation der Daten liefert. Die automatische Verschlüsselung in Abhängigkeit der getroffenen Klassifikation des Datenträgers sowie der festgelegten Strategie bleibt dem Benutzer verborgen, da die Verschlüsselung beim Abspeichern von Daten auf dem Datenträger sowie die Entschlüsselung beim Lesen von Daten von dem Datenträger automatisch erfolgt und dieser Vorgang im Kernel Mode, d.h. für den Benutzer verborgen, durchgeführt wird. Hierdurch wird insbesondere ein Datendiebstahl von solchen Personen effektiv unterbunden, die zwar berechtigt sind, die Daten zu bearbeiten, jedoch keine Berechtigung für eine Weitergabe der Daten haben. Der Einsatz des Verfahrens kann ohne Kenntnis des Benutzers erfolgen.

Weitere Details des Ausführungsbeispiels ergeben sich aus Figur 4. Der Klassifikator 114 überwacht einige oder alle Schnittstellen und Bussysteme über die eine Anschlussmöglichkeit für Datenträger 104 besteht. Der Klassifikator 114 unterscheidet zwischen Datenträgern 104 und anderen Geräten wie Tastatur, Maus, Drucker, Scanner, etc.

Erkannte Datenträger 104 (Volumes) werden hinsichtlich ihres „Gefahrenpotentials“ klassifiziert. Zur Klassifikation werden die deklarierten Eigenschaften, Inhalte, sowie die Einbettung in das Betriebssystem ausgewertet. So wird z.B. das Volume auf dem sich das Betriebssystem befindet anders klassifiziert als ein mittels USB-Schnittstelle nachträglich gemountetes Volume auf einem Memory-Stick; eine Diskette anders als eine Festplatte.

Besonders vorteilhaft ist, dass nicht ein bestimmtes Volume zur Verschlüsselung ausgewählt wird, sondern eine Klasse von Volumes, die beliebig viele Instanzen beinhalten kann. Typ, Inhalt und Verhalten eines jeden Volumes sind die Grundlage für die Klassifikation. Dabei bleibt mit dem erfindungsgemäßen Verfahren die volle Funktionalität der Schnittstellen erhalten, z.B. beim Anschluss eines Druckers an einen USB-Port.

Der Aktivitätsmonitor 113 beobachtet die Kommunikation der Dateisystemtreiber mit den übrigen Komponenten. Er registriert Anforderungen (read/write/seek/ioctl/...) aus dem User Mode 200, z. B: von Diensten oder Anwendungsprogrammen ebenso wie Anforderungen aus dem Kernel Mode 100, z. B. von Cache-Manager 101 oder Memory Manager 102. Die Analyse der Kommunikation ermöglicht die Bildung von zwei disjunkten Klassen, d.h. jede Anforderung lässt sich eindeutig zuordnen. Diese sind:

1. Datentransfer und Funktionen innerhalb des Hauptspeichers,
2. Datentransfer und Funktionen unter Beteiligung eines Datenträgers 104.

Alle Anforderungen der zweiten Klasse müssen das Ver-/Entschlüsselungsmodul 105 passieren und werden dort je nach implementierter Strategie manipuliert. Sie erhalten ein virtuelles Etikett, dessen Information zu der Entscheidung des Ver- bzw. Entschlüsselungsmoduls 105 beitragen, wie mit den Daten dieser Anforderung zu verfahren ist.

Anforderungen, die direkt, d.h. ohne Beteiligung des Datenträgers 104, z.B. aus oder mit dem Cache erledigt werden können, können unverändert passieren.

Indem nur während der ohnehin vergleichsweise langsamen Zugriffe auf Datenträger 104 die Ver- bzw. Entschlüsselung durchgeführt wird, reduziert diese Konzeption den Einfluss auf die Systemleistung auf ein absolutes Minimum. Auch die Ver- bzw. Entschlüsselung erfolgt mit maximaler Effizienz, da nahezu immer Blöcke gleicher Größe bearbeitet werden und der Algorithmus entsprechend optimiert werden kann.

Mittels des Schlüsselmanagers 116 erfolgt die Bereitstellung eines oder mehrerer Schlüssel für die Ver- und Entschlüsselung 105.

In Figur 5 dargestellt ist die Modifikation einer auf einem Speichermedium 104 zu speichernden Datei 50 durch die Verschlüsselung 105 bei Verwendung eines Vorspanns 601 bzw. eines Nachspanns 603, d.h. dass die tatsächlich auf dem Speichermedium 104 abgelegte Datei 60 gegenüber der dem Klienten des

Dateisystems 103 vorliegenden Datei 50 modifiziert ist. Unter dem Klienten des Dateisystems 103 wird insbesondere jedes Anwendungsprogramm sowie jeder Bestandteil des Betriebssystems verstanden, welches sich der Dienste des Dateisystems, wie z.B. Lesen und Schreiben von Dateien, bedient.

Bei Verwendung eines privaten (d. h. nur dem vorgestellten Verfahren dienenden) Vorspanns 601 oder Nachspanns 603 in einer verschlüsselten Datei 60 werden die Dateigrößen um die Größe der zusätzlichen Daten vermindert. Dem Klienten des Dateisystems 103 wird eine entsprechend kleinere Datei 502 „vorgetäuscht“.

Die Verwendung eines privaten Vorspanns 601 in einer verschlüsselten Datei 60 werden die Positionsinformationen durch entsprechende Addition/Subtraktion transformiert. Die dem Klienten des Dateisystems 103 als Dateianfang erscheinende Position in der Datei 50 ist physikalisch auf dem Datenträger 104 die Position unmittelbar nach dem privaten Vorspann 601.

Die Verwendung eines privaten Nachspanns 603 bleibt für den Klienten des Dateisystems 103 in ähnlicher Weise unkenntlich. Das scheinbare Dateiende ist auf dem Datenträger 104 der Beginn des (für den Klienten des Dateisystems 103 unerreichbaren) Nachspanns 603.

Für den Klienten des Dateisystems 103 ist somit lediglich der Dateiname 500 sowie die eigentliche Datei 502 sichtbar, die auch in dieser Form dem Benutzer angezeigt werden. Die tatsächliche, d.h. physikalische Datei 60 auf dem Speichermedium 104 weist jedoch einen modifizierten Dateinamen 600 auf. Des Weiteren ist der Inhalt, d.h. die eigentliche Datei 602 – unabhängig von ihrem inneren Aufbau – gegenüber dem für die Klienten des Dateisystems 103 vorliegenden Dateinhalt 502 modifiziert und um einen Vorspann 601 und/oder einen Nachspann 603 ergänzt.

Für verschlüsselte Dateien 60 wird für alle Operationen mit Bezug auf Dateinamen 600 die Namensraumtransformation durchgeführt.

Für verschlüsselte Dateien 60 wird die Entschlüsselung 105 durchgeführt. Bei fehlendem oder nicht passendem Schlüssel erfolgt eine entsprechende Meldung; der Zugriff bleibt wie bei nicht mit diesem Verfahren arbeitenden Systemen verwehrt, d.h. fehlende Schlüssel führen schon im Aktivitätsmonitor zu den entsprechenden Meldungen. Die Anforderungen erreichen den Dateisystemtreiber gar nicht erst.

Für zu verschlüsselnde Dateien 50 wird die Verschlüsselung 105 durchgeführt. Bei fehlendem Schlüssel ist keine Schreiboperation möglich, d.h. dass auch in diesem Fall fehlende Schlüssel schon im Aktivitätsmonitor zu den entsprechenden Meldungen führen und den Dateisystemtreiber nicht erreichen.

Alle anderen Daten (nicht zu verschlüsselnde Dateien, Metadaten des Dateisystems außer ggf. Dateigrößen) bleiben unverändert. Die spezifischen Vorteile jedes Dateisystems 103 bleiben in vollem Umfang erhalten.

Zur Verschlüsselung 105 können sowohl eine Strom- als auch eine Blockverschlüsselung zur Anwendung kommen. Da blockbasierte Verfahren üblicherweise bessere Ergebnisse liefern, und nahezu alle Daten bereits in Blöcken konstanter Größe vorliegen, bietet sich ihre Verwendung an.

In Figur 6 dargestellt ist ein Ablaufdiagramm, welches das Öffnen bzw. Erstellen einer Datei unter Anwendung des erfindungsgemäßen Verfahrens zeigt, wobei hier die Strategie verfolgt wird, dass ein temporäres Außerkraftsetzen der Verschlüsselung zulässig ist. Es werden sowohl die Berechtigung als auch der Schlüssel überprüft. Bei Vorliegen der Voraussetzungen erfolgt eine „normale“ Betriebsart. Mangelt es an einer der Voraussetzungen, so führt dies zu einer Fehlermeldung, d.h. dass die Daten dem Benutzer verborgen beliben.

In den Figuren 7 und 8 dargestellt ist der Datenfluss beim Lesen und Schreiben einer Datei mit dem erfindungsgemäßen Verfahren gemäß der Darstellung nach Figur 4 unter Berücksichtigung eines Memory-Managers 102 sowie eines Cache-Managers 101 (in Figur 7) bzw. ohne Berücksichtigung eines Memory-Managers

und eines Cache-Managers (in Figur 8). In Figur 9 dargestellt ist der Datenfluss beim Lesen und Schreiben via Memory Mapped Files MMF.

Den Darstellungen nach Figuren 7 bis 9 ist zu entnehmen, dass ein Zugriff auf das Speichermedium 104 unter Berücksichtigung des Klassifikators 114 auf Grund der Implementierung des Verfahrens im Kernel-Mode 100 jeweils ausschließlich unter Berücksichtigung des Ver-, bzw. Entschlüsselungsmoduls 105 möglich ist. Ein Zugriff auf ein Speichermedium 104 an dem Ver-, bzw. Entschlüsselungsmodul 105 vorbei wird zuverlässig unterbunden.

Unabhängig davon, ob bzw. in welcher Form seitens des Betriebssystems ein Memory Manager 102 und ein Cache Manager 101 im Kernel Mode 100 implementiert und in die Interaktion mit dem Dateisystem 103 involviert sind, erfolgt durch den Aktivitätsmonitor 113 und die Verschlüsselung 105 jeweils eine Überwachung des Datenstromes 130, 131 zwischen Dateisystem 103 und dem Speichermedium 104, wobei das Speichermedium 104 durch den Klassifikator 114 hinsichtlich des damit verbundenen Gefahrenpotentials eines Verlustes der Vertraulichkeit der Daten klassifiziert wird. Dabei wird sowohl der Datenstrom 130 vom Dateisystem 103 zu dem Speichermedium 104 hin überwacht und gegebenenfalls in Abhängigkeit der vorgenommenen Klassifikation verschlüsselt als auch wird der Datenstrom 131 vom Speichermedium 104 zum Dateisystem 103 hin überwacht, wobei hier gegebenenfalls eine automatische Entschlüsselung der Daten erfolgt.

In Figur 10 dargestellt ist eine Möglichkeit der Bildung eines Schlüssels 300 aus Domänenanteil 301, einem individuellen Anteil 302 sowie einer Funktion 303. Alle Schlüssel 300 werden aus mehreren Teilen 301, 302, 303 variabler Bitlänge zusammengesetzt. Der Domänenanteil 301 ist für alle Schlüssel einer Domäne gleich und erzeugt den Initialisierungsvektor 4010. Er gewährleistet die Trennung der Sicherheitsdomänen. Seine Länge sollte 128 Bit nicht unterschreiten. Alle Rechner die mit dem vorgeschlagenen Verfahren arbeiten, bilden Sicherheitsdomänen 10. Datentransfer mittels wechselbarer Medien 104 ist nur innerhalb einer Sicherheitsdomäne 10 möglich.

Der individuelle Anteil 302 in Verbindung mit dem Funktionsanteil 303 dient zur Erstellung von gleichschließenden Schlüsseln innerhalb einer Sicherheitsdomäne. Schlüssel 300 die bei gleichem Funktionsanteil 303 gleiche Initialisierungsvektoren 4010, 4020 ergeben, sind äquivalent. Durch geschickte Wahl des individuellen Anteils 302, z.B. durch ein Konfigurationsprogramm, lassen sich Schlüsselgruppen und -hierarchien erstellen.

Der Funktionsanteil 303 kodiert die Funktion des Schlüssels 300 als kryptografischer Schlüssel, Berechtigungsschlüssel, Komplement, etc. Bei einem Komplement n-ter Ordnung bedeutet dies, dass diese n Schlüssel nur zusammen wirksam sind.

Der individuelle Anteil 302 dient zur Unterscheidung und ggf. dem Verwendungsnachweis individueller Schlüssel 300.

Der Schlüsselmanager 116 bezieht die Schlüssel 300 oder einzelne Anteile 301, 302, 303 auf unterschiedlichen Wegen:

- von der Benutzeranmeldung (explizit für diesen Zweck modifiziert, oder transitiv anhand des angemeldeten Benutzers) und/oder
- biometrisch und/oder
- aus einem Hardware Token und/oder
- von einem Schlüsselserver.

Durch Abgleich mit vorgegebenen Profilen können Schlüssel 300 temporär oder permanent modifiziert werden. Beispielsweise kann der in einem verloren gegangenen Token gespeicherte Schlüssel 300 durch seinen individuellen Anteil 302 identifiziert und permanent deaktiviert werden.

Durch eine Zeitsteuerung kann eine weitere Differenzierung vorgenommen und bestimmte Funktionen auf Zeiten entsprechend eines vorgebbaren Zeitraumes begrenzt werden, d.h. hinsichtlich einer maximalen Nutzungsdauer und/oder hinsichtlich zugelassener Zugriffszeiten.

Alternativ zu der Darstellung nach Figur 10 kann der Schlüssel 300 einen Dömanenanteil 301 aufweisen, wobei der individuelle Anteil 302 und/oder die Funktion 303 die Länge Null aufweisen.

Das Vorliegen eines Berechtigungsschlüssels erlaubt einem Anwender, die Verschlüsselung 105 außer Kraft zu setzen. Passender Schlüssel vorausgesetzt, werden bereits verschlüsselte Dateien weiterhin entschlüsselt, Aktualisierungen erfolgen verschlüsselt, aber neu angelegte Dateien werden optional nicht verschlüsselt. In Abhängigkeit von der administrativen Konfiguration sind ggf. weitere Bedingungen zu erfüllen, wie beispielsweise komplementärer Schlüssel, bestimmter Rechner, Datum/Wochentag/Zeit, etc.

Das Ver-/Entschlüsselungsmodul 105 ist im Kommunikationspfad zwischen dem Treiber für das Dateisystem 103 b und dem jeweiligen Treiber für den betreffenden Datenträger 104 angeordnet. Es sorgt für die Ver- und Entschlüsselung gemäß der implementierten Strategie und transformiert alle notwendigen Parameter und Resultate in der Kommunikation so, dass der zu Grunde liegende Datenträger, obgleich ganz oder in Teilen verschlüsselt oder anderweitig modifiziert, für das Dateisystem 103 korrekt gemäß seiner Spezifikation erscheint. Es erstellt on-the-fly (=transparent) quasi einen virtuellen Datenträger und substituiert damit den realen Datenträger 104. Innerhalb einer Sicherheitsdomäne 10 ist die Anwendung des Verfahrens nicht zu bemerken.

Als Verschlüsselungsalgorithmus kann vorteilhaft der Rijndael-Algorithmus AES angewendet werden. Eine signifikante Erhöhung der Sicherheit ergibt sich durch die Verwendung einer Kombination aus einem ersten kryptografischen Algorithmus 401, beispielsweise des Rijndael-Algorithmus AES, mit einem zweiten, nachfolgenden kryptografischen Algorithmus 402. Die Sicherheit erhöht sich damit wesentlich, da als Eingangswert für den nachfolgenden Algorithmus bereits randomisierte Daten dienen. Damit potenziert sich der Aufwand für die statistische Kryptoanalyse.

Die Positionierung der Ver- bzw. Entschlüsselung an der vorgesehenen Stelle vor bzw. nach sämtlicher Verarbeitung durch den Dateisystemtreiber bietet weitere Vorteile:

- Die Verschlüsselung erzeugt Daten, die eine nachfolgende Datenkompression nicht mehr zulassen. Eine vorausgehende Datenkompression durch den Dateisystemtreiber (z.B. NTFS) bleibt davon unberührt.
- Metadaten wie z.B. das Verzeichnis der belegten/freien Blöcke bleiben -je nach Strategie - für alle oder zumindest für Rechner die mit dem vorgeschlagenen Verfahren arbeitet unverschlüsselt. Damit bleiben alle Diagnose- und Reparaturmöglichkeiten erhalten.
- Die Blockstruktur der Datenträger korreliert mit der Datenstruktur der stärkeren, blockorientierten kryptografischen Verfahren.
- Die volle Kompatibilität zu Memory Mapped Files bleibt gewahrt. MMFs stellen eine sehr effiziente Methode für den Dateizugriff dar. Im virtuellen Adressraum eines Prozesses wird in einem Bereich eine Datei (ganz oder in Teilen) eingeblendet. Beim Zugriff auf eine Adresse dieses Bereichs wird ein Seitenfehler ausgelöst und dieser entsprechende Bereich mit Arbeitsspeicher hinterlegt, der mit Blöcken aus der Datei gefüllt wird. Im Falle einer Veränderung werden veränderte Blöcke entweder unmittelbar nach expliziter Anforderung oder zeitverzögert automatisch wieder in die Datei zurückgeschrieben.
- Die Beeinträchtigung der Systemleistung wird minimiert. Die Ver- und Entschlüsselung findet nahezu ausschließlich zu den Zeiten statt wo ansonsten ungenutzte Prozessorzeit zur Verfügung steht (Warten auf I/O) von Datenträgern.

Weiterhin implementiert das Ver-/Entschlüsselungsmodul die gewünschte Strategie. Es bestehen die Möglichkeiten der Verschlüsselung des Datenträgers in toto, d.h. jeder Block wird verschlüsselt oder der Verschlüsselung aller Dateien oder der Verschlüsselung einiger Dateien.

Ansprüche

1. Verfahren zur Verhinderung des Verlustes der Vertraulichkeit der in einem Computersystem (11, 12, 13) elektronisch gespeicherten Daten, wobei die Daten insbesondere mittels eines Dateisystems (103) verwaltet werden und/oder eine Einteilung in Blöcke erfolgt, insbesondere bei Verwendung wechselbarer und/oder austauschbarer Datenträger und/oder Speichermedien (104), wobei an das Computersystem (11, 12, 13) insbesondere Peripheriegeräte anschließbar sind, gekennzeichnet durch die Schritte:
 - Analyse des Protokolls und des Datenstromes (130, 131) von und zu Datenträgern und/oder Speichermedien (104) und/oder Peripheriegeräten;
 - Bildung einer Klassifikation, insbesondere zur Unterscheidung zwischen nicht wechselbaren sowie wechselbaren Datenträgern und/oder Speichermedien (104);
 - Festlegung in Abhängigkeit der getroffenen Klassifikation, ob eine Verschlüsselung der elektronisch gespeicherten Daten zur Verhinderung des Verlustes der Vertraulichkeit der Daten erforderlich ist und in Abhängigkeit dieser Festlegung gegebenenfalls
 - Ergänzen des Dateisystems auf einem wechselbaren Datenträger und/oder einem wechselbaren Speichermedium (104) um eine kryptografische Verschlüsselung (601, 602, 603) und/oder Durchführung einer kryptografischen Verschlüsselung aller oder einiger Blöcke des wechselbaren Datenträgers und/oder des wechselbaren Speichermediums (104).
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass festlegbar ist, dass eine Verschlüsselung (105) aller Blöcke des Datenträgers / Speichermediums (104) oder dass eine Verschlüsselung (105) aller Dateien (50) vor der Speicherung auf dem Datenträger / Speichermedium (104) oder dass eine Verschlüsselung (105) einiger Dateien (50) vor der Speicherung auf dem Datenträger / Speichermedium (104) erfolgt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass jedes Dateisystem (103) auf nicht wechselbaren und/oder nicht austauschbaren Datenträgern und/oder Speichermedien (104) um eine kryptografische Verschlüsselung ergänzt wird.
4. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die kryptografische Verschlüsselung (105) bei Vorliegen besonderer Merkmale temporär außer Kraft gesetzt wird.
5. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei Verwendung eines Datenträgers und/oder eines Speichermediums (104) ohne Dateisystem eine Verschlüsselung aller Blöcke erfolgt oder ein Zugriff unterbunden wird.
6. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass eine Verschlüsselung (105) bei Verwendung wechselbarer Datenträger und/oder wechselbarer Speichermedien (104), insbesondere Disketten, Memory-Sticks, CD-RW, DVD-RW und dergleichen, erfolgt.
7. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass eine Verschlüsselung (105) bei Verwendung nicht wechselbarer Datenträger und/oder nicht wechselbarer Speichermedien (104) und/oder netzwerkbasierten Datenträgern und/oder netzwerkbasierten Speichermedien (104) erfolgt.
8. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei Anschluss eines Datenträgers und/oder Speichermediums (104) an eine multifunktionale Schnittstelle und/oder einen multifunktionalen Bus, insbesondere Steckplatz, USB-Port und dergleichen, die Schnittstellen- und/oder Bus-Funktionalität erhalten bleibt und nur derartige Datenströme (130, 131) zumindest teilweise einer Verschlüsselung (105) unterworfen werden, die zur Abspeicherung der Daten an die Schnittstelle und/oder den Bus weitergeleitet werden.

9. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass eine Analyse der Schnittstelle und/oder des Busses erfolgt, an die/den ein Datenstrom (130, 131) erfolgen soll, und diese bei der Bildung der Klassifikation anhand festlegbarer Kriterien berücksichtigt wird, insbesondere hinsichtlich der physikalischen Verbindung und/oder der Geräteeigenschaften.
10. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass kryptografische Methoden zur Verschlüsselung, insbesondere der Rijndael-Algorithmus, angewendet werden.
11. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass die Verschlüsselung in mehreren Stufen erfolgt, insbesondere dass nach Anwendung einer ersten kryptografischen Methode die hierdurch verschlüsselten Daten mittels einer zweiten kryptografischen Methode nochmals verschlüsselt werden.
12. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei einem Lesevorgang von einem zumindest teilweise verschlüsselten Datenträger und/oder Speichermedium (104) eine Entschlüsselung der Daten erfolgt.
13. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass unter Verwendung einer Hardware mit eingebundenem Schlüssel und/oder unter Verwendung eines Kennwortes und/oder durch Erkennung und Überprüfung biometrischer Daten eines Benutzers eine Verschlüsselung (105) von Daten unterbindbar ist.
14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass die Verschlüsselung (105) nur zu festlegbaren Zeiten unterbindbar ist.
15. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass zur Verschlüsselung (105) Schlüssel (300) Verwendung finden, die durch Zusammensetzung verschiedener Anteile (301, 302, 303) gebildet sind, wobei

insbesondere mehrere Computersysteme (11, 12, 13) zu Gruppen (10) zusammengefasst werden, wobei die Schlüssel (300) einer Gruppe (10) von Computersystemen (11, 12, 13) einen übereinstimmenden Anteil (301) sowie jeweils einen individuellen Anteil (302) aufweisen.

16. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass der zur Ver- und Entschlüsselung (105) anzuwendende Schlüssel (300) festlegbar ist und/oder in einer Datenbank abrufbar gespeichert ist und/oder in einer Hardware eingebunden ist und/oder aus biometrischen Daten eines Benutzers unter Verwendung eines Algorithmus ermittelt wird.
17. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass mittels des Computersystems (11, 12, 13) durchgeführte Aktionen wie Abspeichern und/oder Einlesen von Daten protokolliert werden.
18. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass das Computersystem (11, 12, 13) ein Betriebssystem aufweist, das zumindest zwischen einem Kernel Mode (100) und einem User Mode (200) unterscheidet, wobei das Verfahren zumindest teilweise im Kernel Mode (100) implementiert ist.
19. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass ein logischer Zusammenschluss mehrerer Computersysteme (11, 12, 13) zu einer Gruppe (10) erfolgt, wobei innerhalb der Gruppe (10) die kryptografische Verschlüsselung (105) wechselseitig aufgehoben wird, wobei die kryptografische Verschlüsselung (105) nach außen hin aufrecht erhalten wird.
20. Verfahren nach einem der vorherigen Ansprüche, dadurch gekennzeichnet, dass bei Zugriff auf einen Datenträger und/oder Speichermedium (104) eine Prüfung erfolgt, ob eine Verschlüsselung (105) aller Blöcke des Datenträgers / Speichermediums (104) oder eine Verschlüsselung (105) aller Dateien (50) auf dem Datenträger / Speichermedium (104) oder eine Verschlüsselung (105) einiger Dateien (50) vorliegt, und dass eine Entschlüsselung der angeforderten Daten erfolgt.

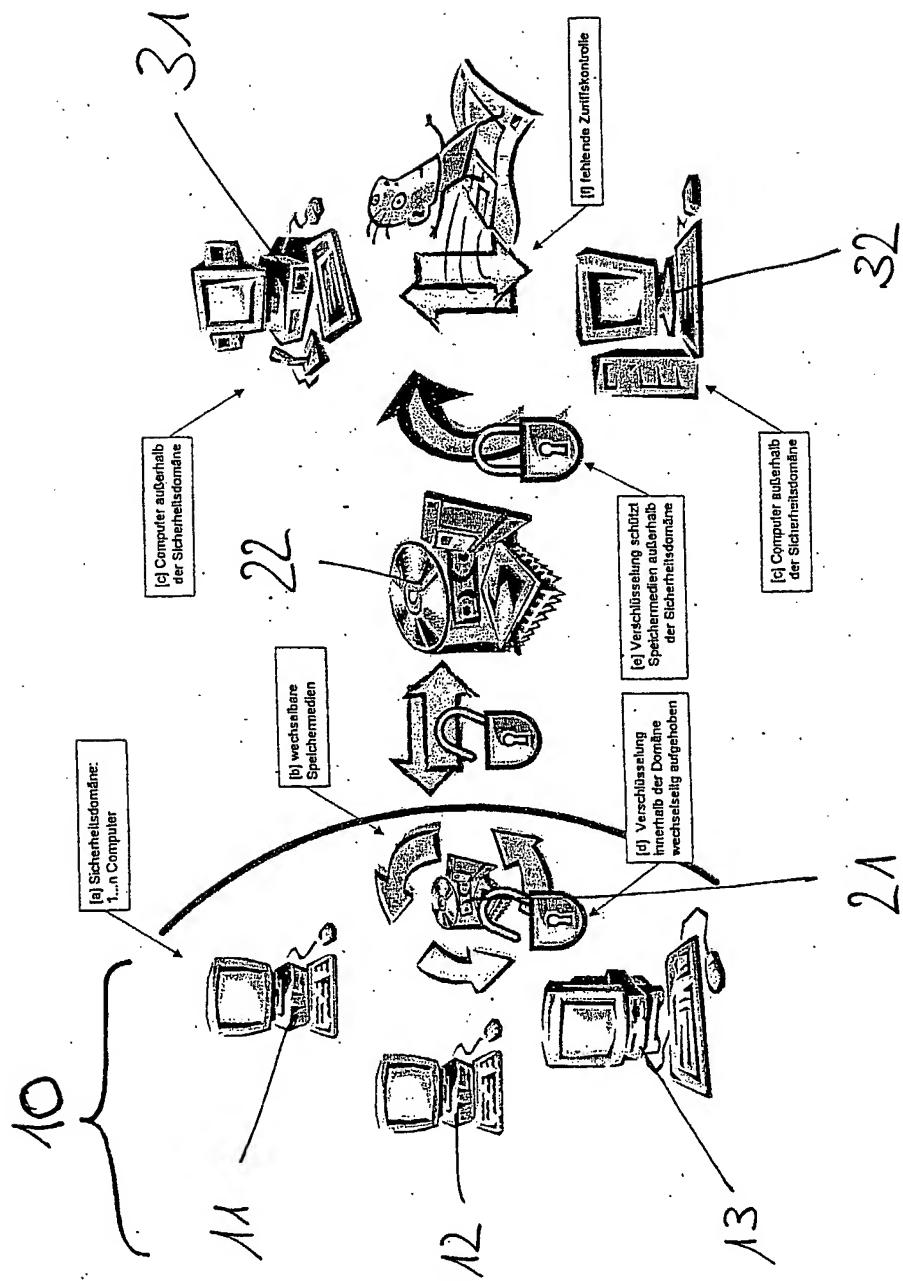


Fig. 1

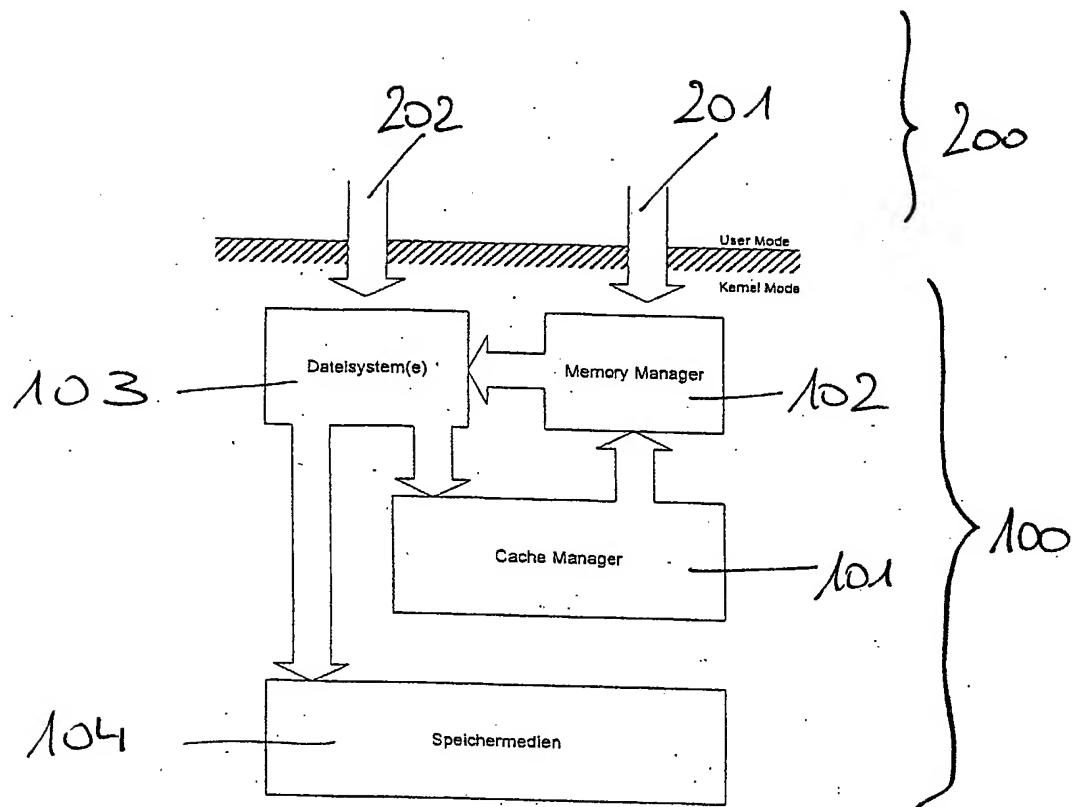


Fig. 2

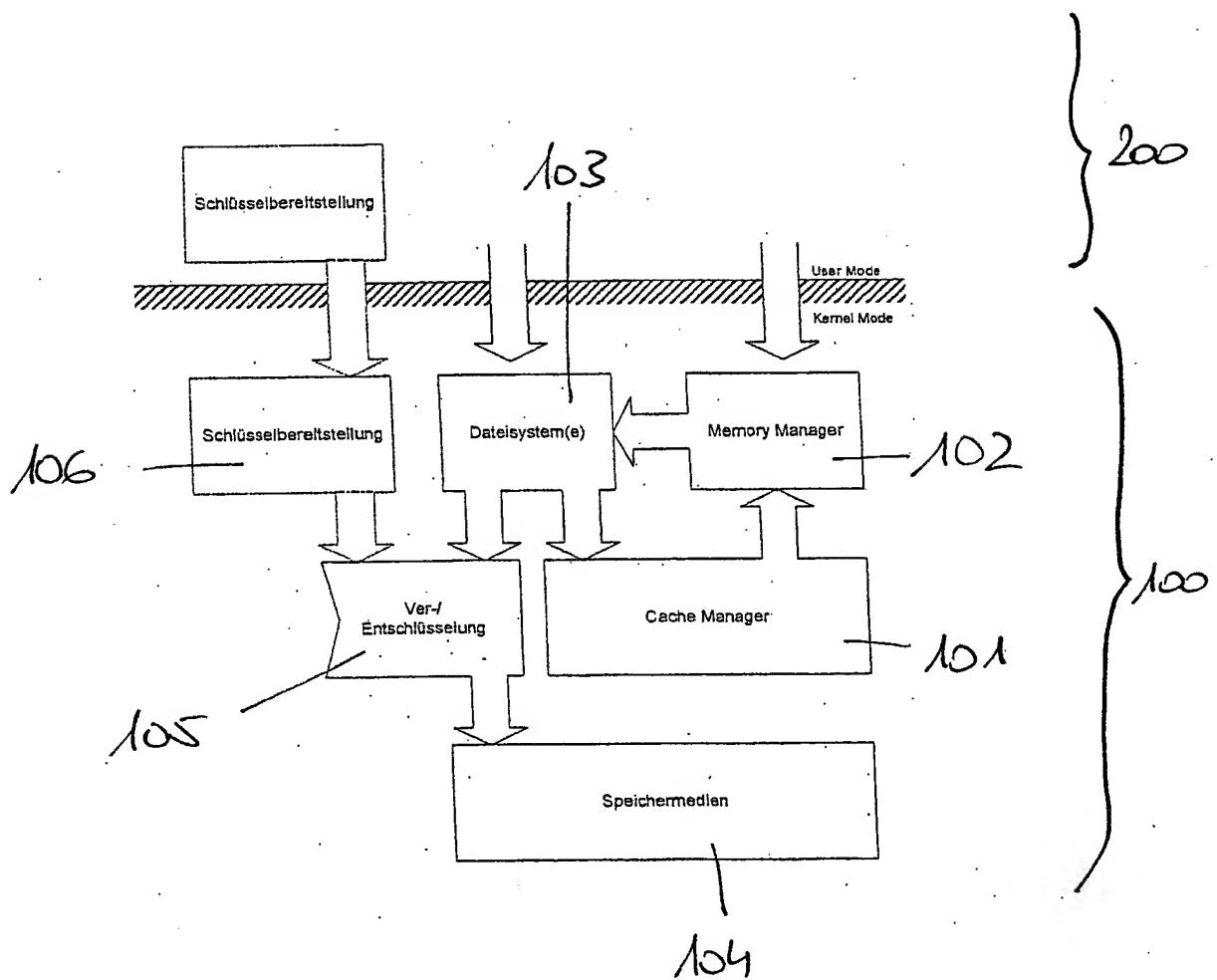


Fig. 3

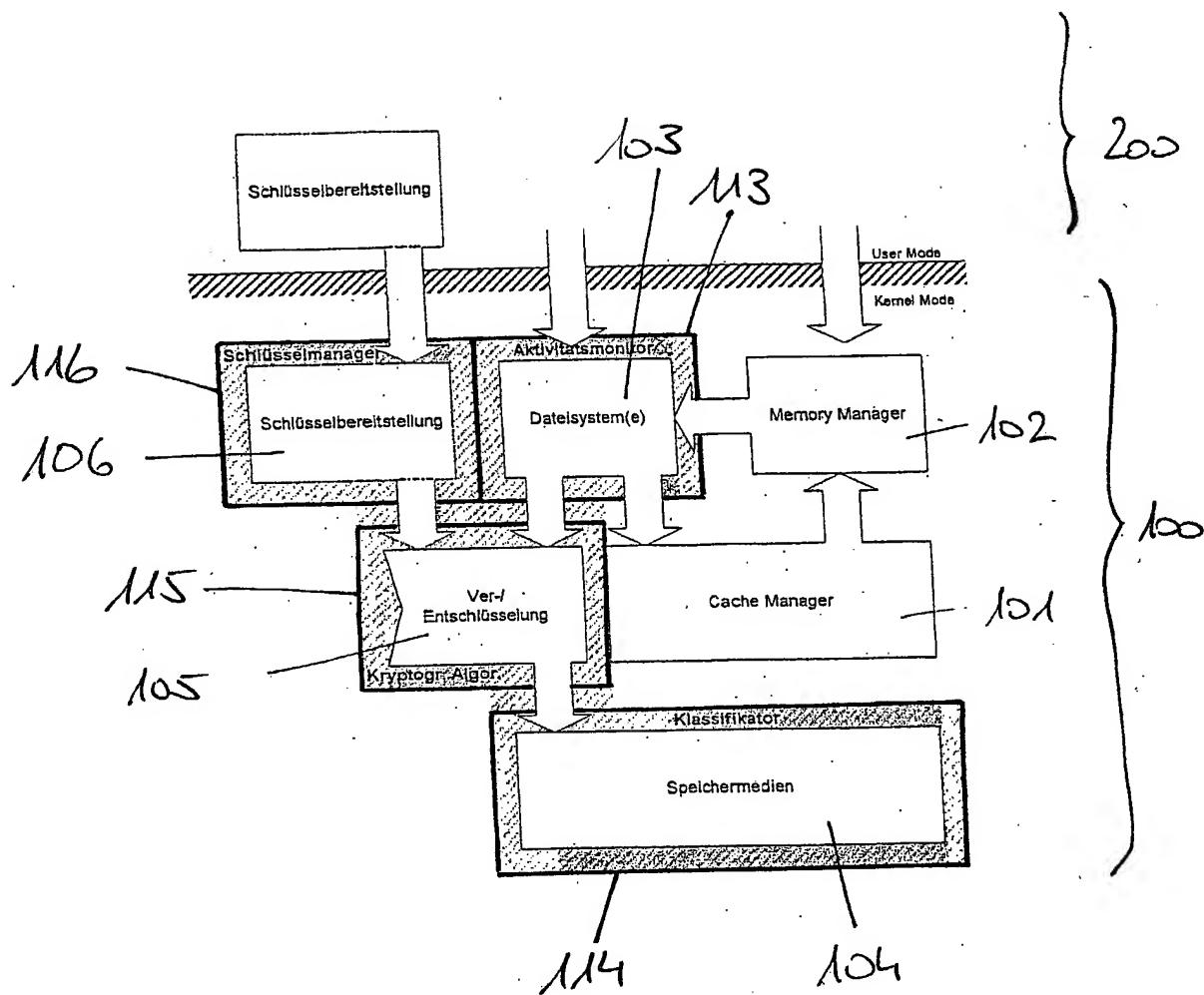


Fig. 4

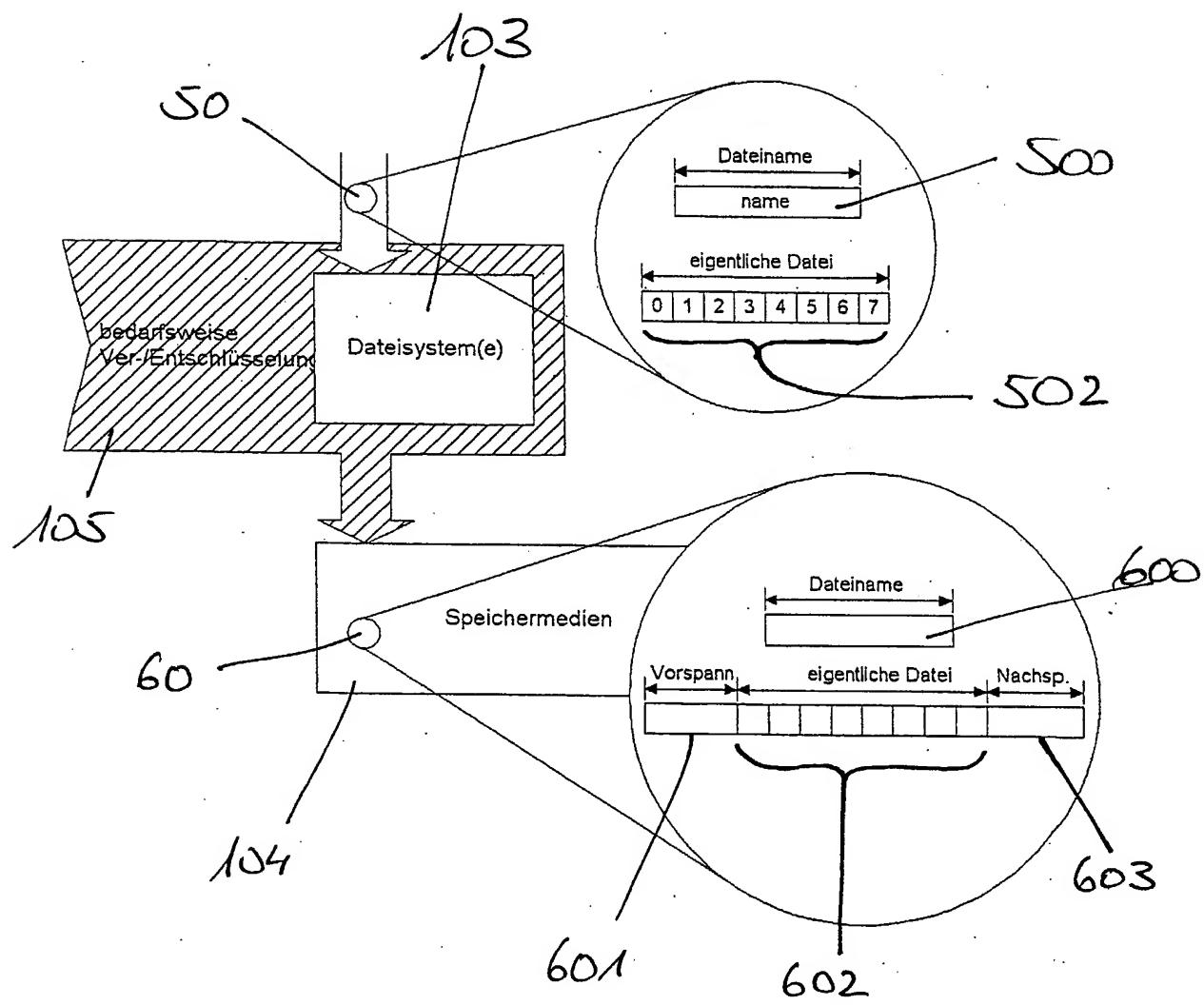


Fig. 5

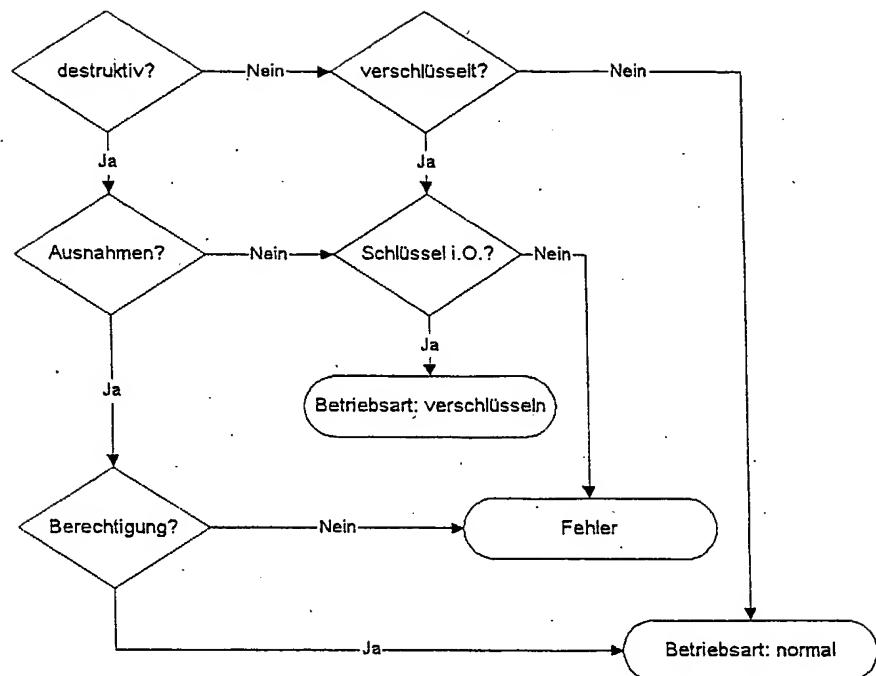


Fig. 6

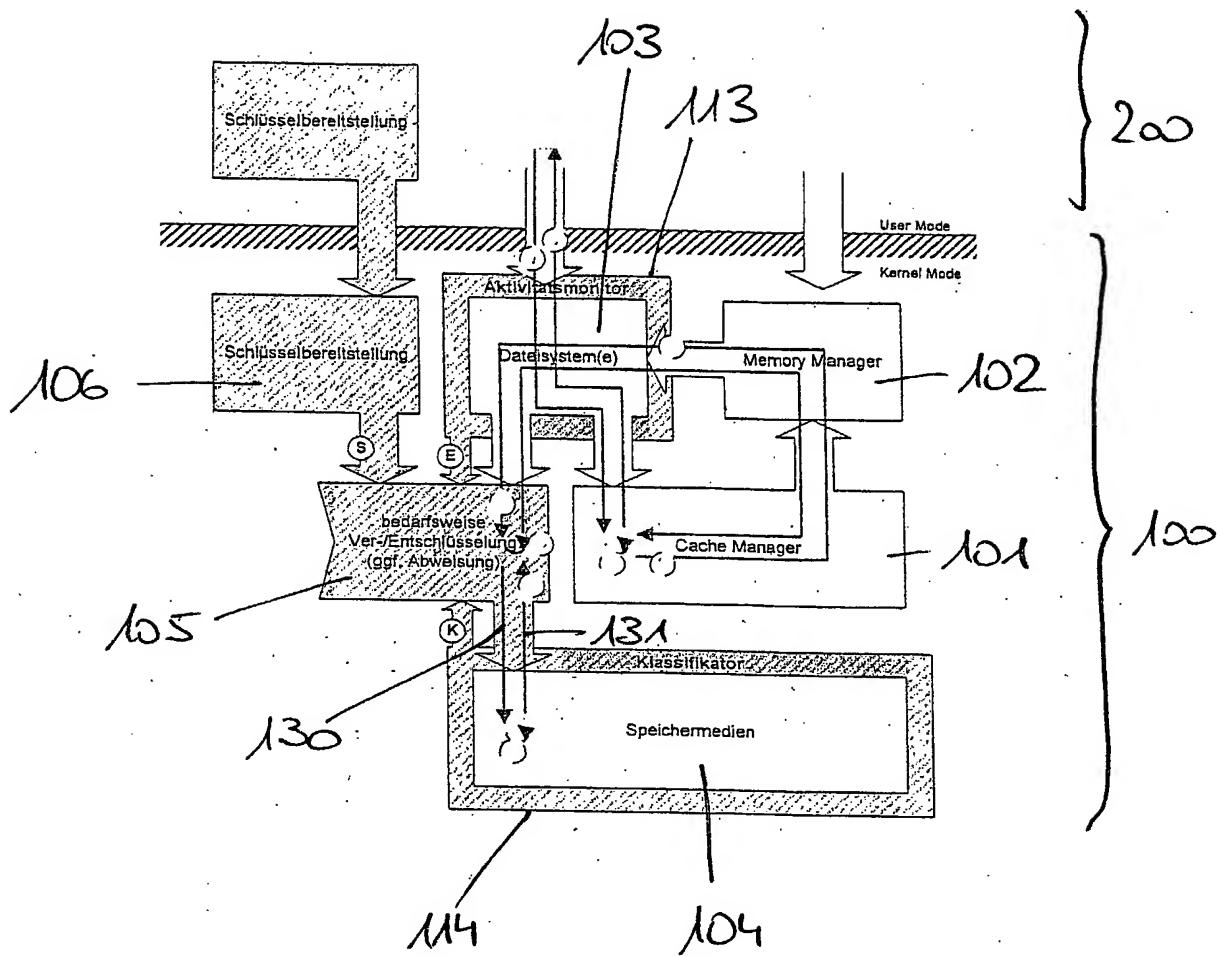


Fig. 7

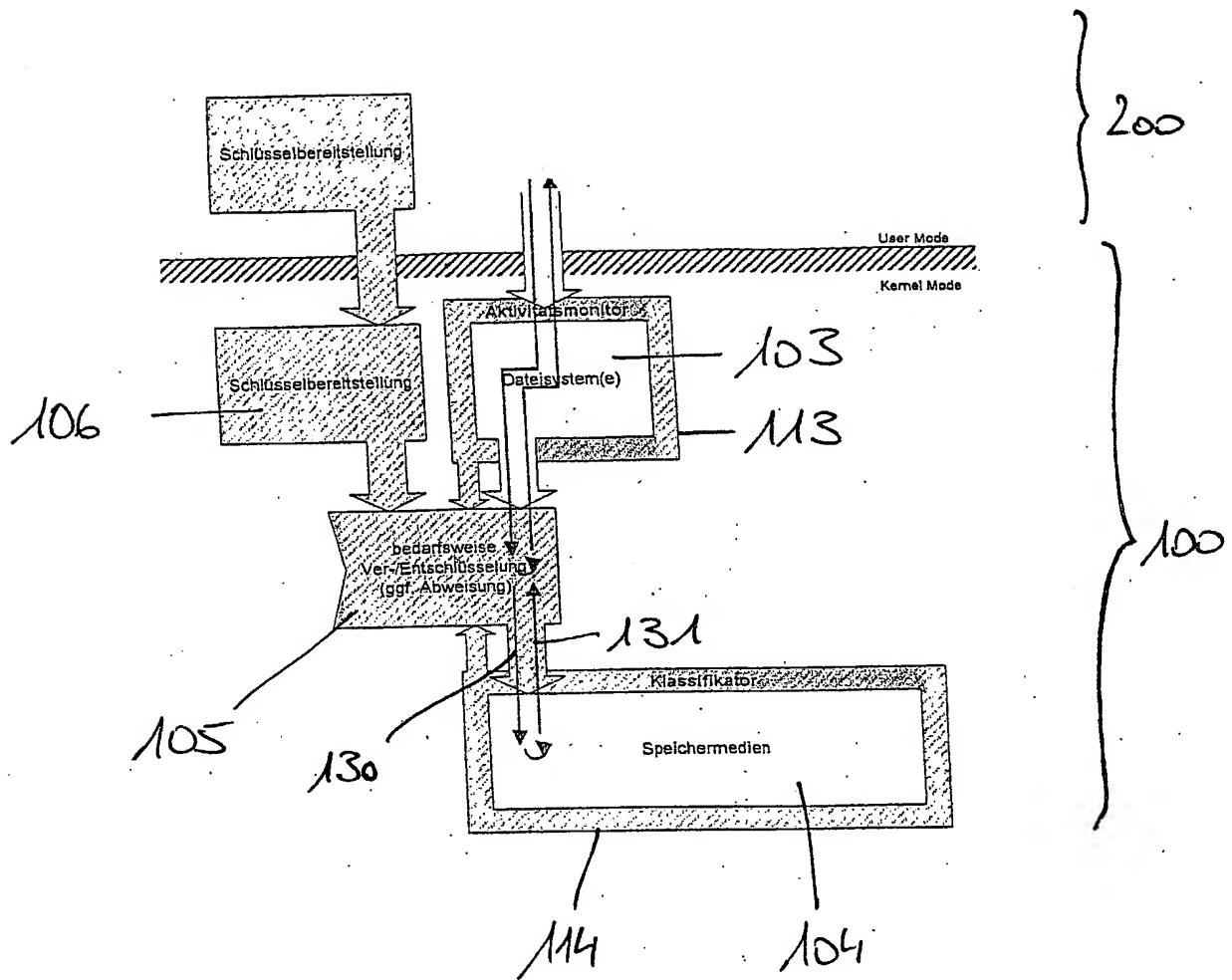


Fig. 8

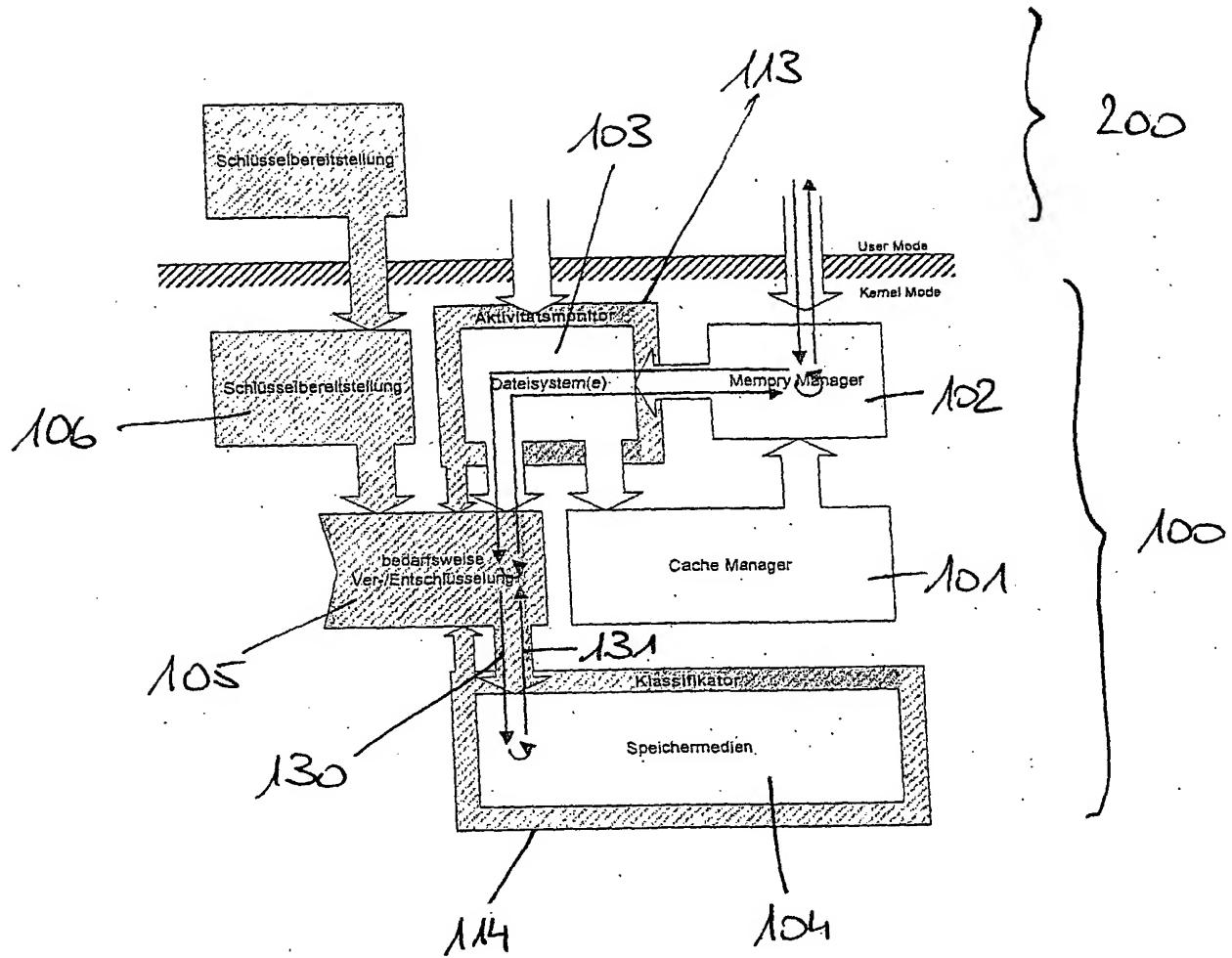


fig. 9

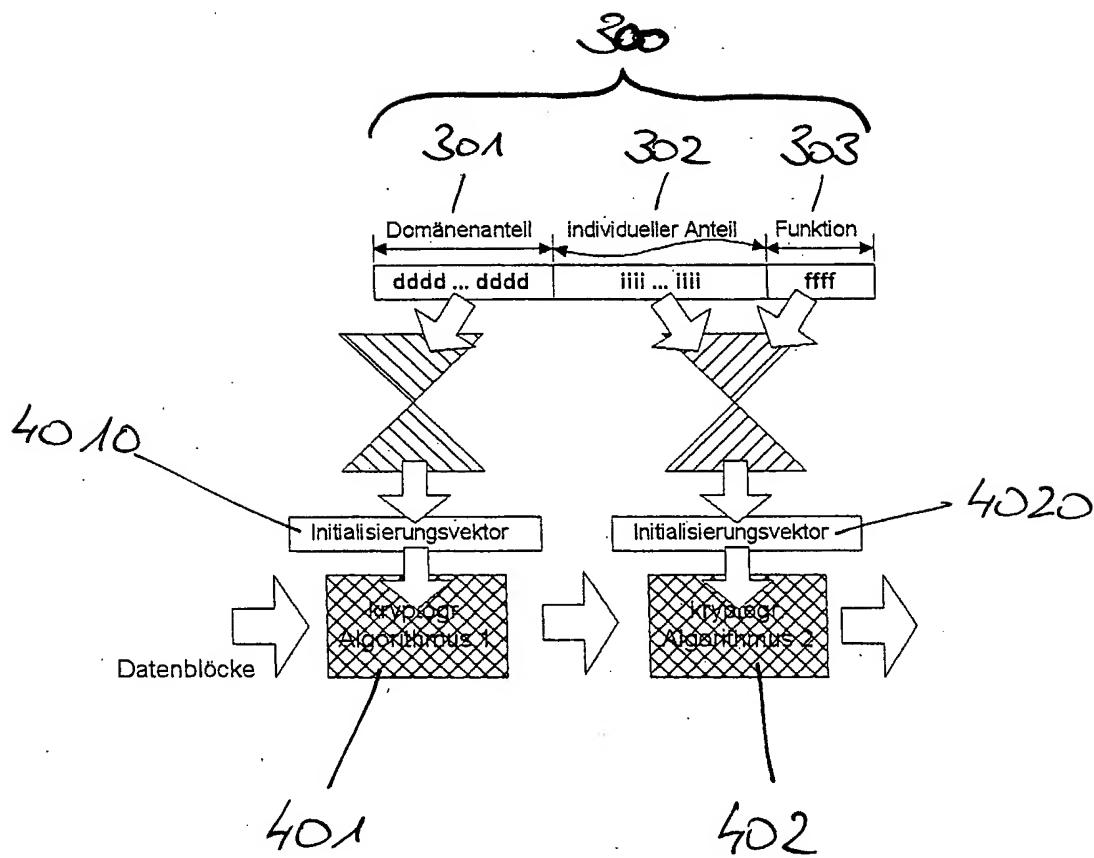


Fig. 10

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP2005/001817

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>ULTIMACO SAFEWARE AG: "SafeGuard Easy – The electronic Fortress – Access Protection and encryption for data on notebooks and workstations" 'Online! March 2003 (2003-03), pages 1-17, XP002328795 Retrieved from the Internet: URL:http://www.conseils.fi/SGEasy_The_electronic_fortress_2003.pdf> 'retrieved on 2005-05-19! page 6 pages 13-15</p> <p>-----</p> <p style="text-align: center;">-/-</p>	1-20

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

° Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

20 May 2005

08/06/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Fleckinger, C

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/001817

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Verschwunden in wenigen Sekunden" NETWORK COMPUTING, REAL-WORLD LABS, 'Online! 10 April 2003 (2003-04-10), pages 14-18, XP002328606 Retrieved from the Internet: URL: http://www.utimaco.de/content_pdf/sieger.pdf > 'retrieved on 2005-05-18! page 16 - page 18 -----	1-20
A	WO 02/19592 A (PARK, TAE-KYOU; IM, YEON-HO; JO, IN-GU) 7 March 2002 (2002-03-07) cited in the application pages 2-3 -----	1-20
A	DAVID BRAUN: "Disk Encryption HOWTO Revision 1.0" NETWORK COMPUTING, 'Online! 30 August 2003 (2003-08-30), XP002328597 Retrieved from the Internet: URL: http://web.archive.org/web/20030830204709/http://ibiblio.org/pub/Linux/docs/HOWTO/other-formats/pdf/Disk-Encryption-HOWTO.pdf > 'retrieved on 2005-05-17! Seite 3, Kapitel 1.6.1 -----	1-20
A	BILL OLIVER, WINMAGIC IN.: "SecureDoc Cryptographic Engine V3.2 - Security Policy" , 1 April 2002 (2002-04-01), XP002328806 page 5 -----	18
A	US 6 009 518 A (SHIAKALLIS ET AL) 28 December 1999 (1999-12-28) columns 2-4 -----	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP2005/001817

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 0219592	A 07-03-2002	KR 2002016701 A		06-03-2002
		AU 3616601 A		13-03-2002
		WO 0219592 A2		07-03-2002
US 6009518	A 28-12-1999	NONE		

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP2005/001817

A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, PAJ, WPI Data

C. ALS WESENTLICH ANGESEHENDE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	<p>ULTIMACO SAFEWARE AG: "SafeGuard Easy – The electronic Fortress – Access Protection and encryption for data on notebooks and workstations" 'Online! März 2003 (2003-03), Seiten 1-17, XP002328795</p> <p>Gefunden im Internet: URL:http://www.conseils.fi/SGEasy_The_electronic_fortress_2003.pdf</p> <p>'gefunden am 2005-05-19!</p> <p>Seite 6 Seiten 13-15</p> <p>-----</p> <p>-/-</p>	1-20

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

Siehe Anhang Patentfamilie

- * Besondere Kategorien von angegebenen Veröffentlichungen :
- *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
- *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
- *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
- *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
- *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

- *T* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
- *X* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
- *Y* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
- *&* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

Absendedatum des internationalen Recherchenberichts

20. Mai 2005

08/06/2005

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Fleckinger, C

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen PCT/EP2005/001817

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	"Vergewussten in wenigen Sekunden" NETWORK COMPUTING, REAL-WORLD LABS, 'Online! 10. April 2003 (2003-04-10), Seiten 14-18, XP002328606 Gefunden im Internet: URL: http://www.utimaco.de/content_pdf/sieger.pdf > 'gefunden am 2005-05-18! Seite 16 - Seite 18 -----	1-20
A	WO 02/19592 A (PARK, TAE-KYOU; IM, YEON-HO; JO, IN-GU) 7. März 2002 (2002-03-07) in der Anmeldung erwähnt Seiten 2-3 -----	1-20
A	DAVID BRAUN: "Disk Encryption HOWTO Revision 1.0" NETWORK COMPUTING, 'Online! 30. August 2003 (2003-08-30), XP002328597 Gefunden im Internet: URL: http://web.archive.org/web/20030830204709/http://ibiblio.org/pub/Linux/docs/HOWTO/other-formats/pdf/Disk-Encryption-HOWTO.pdf > 'gefunden am 2005-05-17! Seite 3, Kapitel 1.6.1 -----	1-20
A	BILL OLIVER, WINMAGIC IN.: "SecureDoc Cryptographic Engine V3.2 - Security Policy" , 1. April 2002 (2002-04-01), XP002328806 Seite 5 -----	18
A	US 6 009 518 A (SHIAKALLIS ET AL) 28. Dezember 1999 (1999-12-28) Spalten 2-4 -----	1

INTERNATIONALES RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2005/001817

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0219592	A 07-03-2002	KR 2002016701 A	06-03-2002
		AU 3616601 A	13-03-2002
		WO 0219592 A2	07-03-2002
US 6009518	A 28-12-1999	KEINE	